Client case study

How a prominent medical facility built a healthy cybersecurity program

EY and a large medical provider team up to reduce cyber risk and better protect patient data.

The better the question

How can a health provider better prevent and treat cyber threats?

Optimized cyber technology is critical to effective threat detection and response.

1

Health providers depend on technology to bridge communications and improve outcomes for patients. Electronic health records, smartphones and tablets, patient portals, remote monitoring capabilities, and virtual visits are advancements that have improved access to health care.

But the convenience of cloud- and web-based applications can come with side effects, including increased exposure to cyber threats.

A major cancer treatment center and academic medical facility with a Level 1 trauma center is actively engaged in efforts to protect medical and patient information from cyber risks.

Currently, this notable health center provides more than 2 million people annually with the high-quality, cutting-edge care the local community expects and deserves. They also recognize that their responsibility doesn't stop with medical care. Ensuring patients' personal health data is safe and secure by staying a step ahead and investing in cybersecurity is also critical.

The personal, reputational and financial damage caused by cyber breaches has made potential exposure to cyber attacks a concern for CISOs in the health and life sciences industry. That's why, for the past five years, this major medical provider and the Ernst & Young LLP (EY) Cybersecurity Managed Services team have been working side-by-side to optimize the health provider's cybersecurity investments for the benefit of its patients and business.

According to the EY 2023 Global Cybersecurity Leadership Insights Study, cyber breaches can account for more than 12% of an organization's overall annual spend on cybersecurity, taking up to eight months to detect and resolve. And health care continues to experience among the highest data breach costs of all industries. In fact, IBM's 2023 Cost of Data Report said the average cost of a data breach in health care has increased 53% over the last three years, jumping from an average of $10 million in 2022 to nearly $11 million in 2023.

EY
Shape the future with confidence

splunk> a cisco company

CROWDSTRIKE

The better the answer

Cyber health starts with 24/7 visibility and risk reduction

EY cyber managed services mitigate risk by helping hospitals detect and respond to cyber incidents.

2

Large health care systems have thousands of interconnected endpoints, from computers to monitors and patient medical devices, creating a potential attack surface area that health care providers need to be able to monitor and protect.

"A strong cyber defense program should proactively monitor for signals of a threat and quickly respond to suspicious activity to contain cyber incidents before business-critical functions are disrupted," says Jennifer Pope, Ernst & Young LLP Partner and account lead. "Working together, we were able to optimize cyber investments to improve this organization's detection and response to cyber attacks."

Endpoint detection and response (EDR) tools enable a behavior-based approach to identify and observe potential cyber threats occurring on user endpoints and servers. The behavior-based EDR tool implemented by EY and the provider organization helps them distinguish malignant attacker activity from benign, but risky, behaviors.

"We also added EY custom detection logic and proactive, intelligence-driven threat hunting capabilities leveraging our EY Alliance partners Splunk and CrowdStrike. And we collaborated on the development of 24/7 real-time reporting dashboards," said Vivek Ashar, Ernst & Young LLP Senior Manager. "Now the health care center has customized, instantaneous information at their fingertips that provides their CISO and cyber teams with increased line of sight into threats."

EY teams helped the health care provider extend threat detection visibility using Splunk, a versatile cybersecurity tool that enables extensive log source integration, analytics and dashboarding, providing an effective and efficient way to sift through large data sets in search of possible threats. The EY Managed Threat Detection and Response service configures and deploys its detection logic from its Attack Intelligence Lab to technologies such as Splunk and CrowdStrike, providing the hospital with 24x7x365 monitoring, alert triage, and attack disruption.

By proactively taking steps to reduce the organization's cyber risk exposure and ramping up its response systems, the health care center is demonstrating its commitment to patient care and data privacy. Leveraging the right mix and application of technology and cyber expertise, the provider can make more informed, data-driven decisions to better safeguard its patients, network and data.

"Our experienced health care cyber professionals sit shoulder-to-shoulder with our clients," adds Pope. "We don't apply a one-size-fits-all approach. Our EY team is a member of your team, and we work to understand your organization so we can deliver personalized support and tailored solutions."

In addition to teaming with the medical provider to optimize the cyber tech stack, EY teams also helped reduce manual efforts related to incident response and expedited attack disruption using Splunk's Security, Orchestration, Automation and Response (SOAR) tool. SOAR enables faster incident response times while reducing administrative burden on the internal cyber response team to complete routine tasks such as resetting passwords, phishing analysis, disabling accounts, and malware removal, thereby allowing them to focus on more long-term, strategic cyber initiatives.

"It's no secret there's a shortage of cyber talent in the marketplace, and that puts a huge burden on in-house teams to fight escalating cyber threats with limited resources," says Tapan Shah, EY US Cybersecurity Managed Services Leader and the lead Principal on the collaboration. "Managed services can offer experienced professionals without the cost of hiring a large team of full-time employees. We can help our clients implement automation and optimize commercial technology investments — expediting and sustaining transformative and mature cyber defenses in a cost-effective manner."

The better the world works

Reducing risky behaviors results in better data protection

An increased threat detection and response program keeps a major health care provider thriving.

3

Together, this client and EY practitioners are bringing the best of next-generation security operations center capabilities to medical device monitoring. Integrating monitoring into a unique governance process with tactical alerting, triage and ticketing capabilities all for the benefit of its more than 2 million patients annually.

With the newly implemented solutions and highly collaborative approach, this critical regional medical facility is now monitoring more than 25,000 internal devices with 24/7 support from EY. The EY team also tailored the cyber managed services to provide the client with insightful reporting that will help identify, prioritize and drive continuous cyber defense improvements, reduce risky behaviors, and tease out credible signals from noise.

Their collaborative work has resulted in a more than 50% increase in cyber incident detection and remediation estimated at over $80 million in organizational revenue protected.

As cyber attacks become more complex and creative, so must an organization's cyber program and defense capabilities. It takes just one infiltration to bring down a network, but an entire cyber team working together around the clock to prevent it.

View more EY case studies

Contact

Nana Ahwoi
EY Americas Consumer and Health Cybersecurity Industry Leader
Ernst & Young LLP

EY | Building a better working world

EY exists to build a better working world, helping create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

US SCORE no. 23394-241US

2303-4204113
ED None

ey.com